296_Schegge-di-Cassandra--OHM2013--l-hard-disk-vi-guarda

Schegge di Cassandra/ OHM2013: l'hard disk vi guarda

(296) - L'hack di Sprite_TM dimostra come sia possibile accedere a porzioni inesplorate degli hard disk. E riporvi codice di ogni tipo…

Schegge di Cassandra/ OHM2013: l'hard disk vi guarda

Figure 1:

(296) - L'hack di Sprite_TM dimostra come sia possibile accedere a porzioni inesplorate degli hard disk. E riporvi codice di ogni tipo, all'insaputa dell'utente, per gli scopi più terribili.

16 agosto 2013—Cassandra mantiene sempre le promesse, e questa volta la cosa è oltretutto particolarmente facile. "Observe, Hack, Make" non si è ancora cristallizzato nella memoria della

Rete (video e slide non sono ancora disponibili sul sito), ma il ricordo di questo divino seminario, “Hard Disk: molto più che semplici device a blocchi”, tenuto da Jeroen Domburg *aka* “Sprite_TM”, cioè la persona dietro il noto sito di hacking Spritesmods.com, esige inesorabilmente di essere messo subito nero su bianco.

In attesa quindi che sul sito di OHM2013, in fondo alla pagina dell’intervento compaiano le slide scaricabili o il video dell’intervento (tutti i seminari sono stati videoregistrati), Cassandra cercherà di riassumere non i tecnicismi, ma la meraviglia che questi le hanno suscitato.

Sprite_TM ha infatti già pubblicato un ottimo articolo che contiene tutti i dettagli tecnici: i lettori più competenti potranno perciò fermarsi qui ed abbeverarsi direttamente alla fonte della conoscenza.

Per le persone normali invece Cassandra riassumerà, in termini più usuali il contenuto del seminario.

Ripartiamo quindi dall’inizio: già nel 2005 anche un vecchio articolo di Cassandra profetava come l’industria dell’elettronica di consumo sfornasse oggetti che, oltre alla loro funzione primaria, contenevano risorse informatiche che permettevano di realizzare) funzionalità “nascoste” agli utenti normali, come ad esempio la profilazione pubblicitaria o una geolocalizzazione silente.

Dal 2005 tuttavia molta acqua è passata sotto i ponti, e molta strada è stata percorsa dall’industria elettronica. Consideriamo ad esempio un moderno hard disk da due Terabyte, che si compra ormai a meno di 100 euro ovunque. Visto nudo e crudo è un parallelepipedo di metallo con un circuito stampato da una parte ed una coppia di connettori dietro. Se collegato con un cavo chiamato SATA (Serial-ATA) ad un computer ed inserito dentro di esso, permette di installarvi sopra un sistema operativo e memorizzarvi un sacco di file di vario tipo. Tutto qui? Ovviamente no.

Innanzitutto, da sempre, in tutti i device elettronici sono presenti, per motivi tecnici non maliziosi, modalità nascoste di accesso che permettono di aggiornare il firmware od eseguire operazioni diagnostiche. Spesso sul circuito stampato sono presenti aree inutilizzate dove è però possibile saldare una porta seriale, USB o una più moderna JTAG che non essendo fisicamente installate non sono utilizzabili dal loro proprietario… a meno che non sia un hacker.

In quest’ultimo caso l’esame di particolare modello di un hard disk da 2 TB permette di vedere che sul circuito stampato sono presenti appunto una porta seriale ed una porta JTAG.

Saldati sul circuito stampato fanno poi bella mostra di sé un chip RAM da 64 Megabytes, una ROM contenente fino 256 Kb di firmware, cioè il software “nascosto” che controlla e fa funzionare l’hard disk, ed infine non una, non due ma dicasi tre CPU, inserite un un unico chip, quello del “controller” dell’hard disk stesso.

Molto rozzamente, si potrebbe dire che dentro l’hard disk in questione ci sono tre computer, computer molto semplici, ma tre.

L’autore del seminario ha cercato informazioni in Rete, informazioni che le industrie elettroniche si guardano bene dal rendere pubbliche, ma che filtrano inevitabilmente nei forum e nelle mail list, ha saldato gli opportuni fili negli opportuni posti del circuito stampato dell’hard disk, e si è poi collegato ad esso sia via porta seriale che JTAG. Con un paziente ma nemmeno troppo lungo lavoro, durato 2 o 3 settimane, ha decodificato il funzionamento del firmware, si è accorto che una delle 3 CPU era praticamente sempre disoccupata, ed ha realizzato dei firmware modificati con “capacità nascoste”.
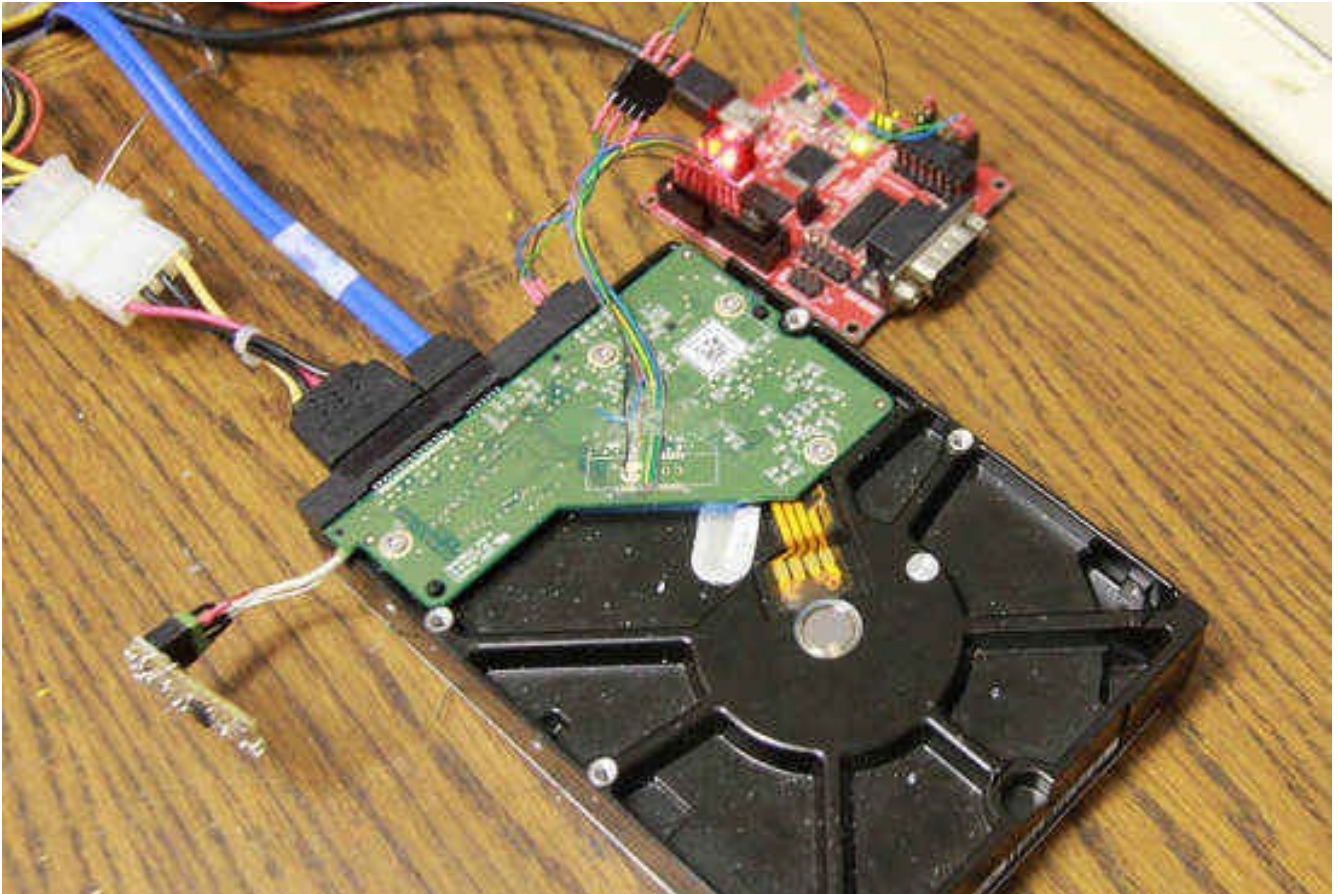
Figure 2:

```
ROXTerm
jeroen@spritesws:~/hddfw$ openocd
Open On-Chip Debugger 0.8.0-dev-00026-g45bafc5 (2013-06-12-09:54)
Licensed under GNU GPL v2
For bug reports, read
        http://openocd.sourceforge.net/doc/doxygen/bugs.html
Info : only one transport option; autoselect 'jtag'
adapter speed: 1000 kHz
trst_only separate trst_push_pull
force soft breakpoints
x
Info : max TCK change to: 30000 kHz
Info : clock speed 1000 kHz
Warn : There are no enabled taps.  AUTO PROBING MIGHT NOT WORK!!
Warn : AUTO auto0.tap - use "jtag newtap auto0 tap -expected-id 0x4ba00477
 ..."
Warn : AUTO auto1.tap - use "jtag newtap auto1 tap -expected-id 0x140003d3
 ..."
Warn : AUTO auto2.tap - use "jtag newtap auto2 tap -expected-id 0x140003d3
 ..."
Warn : AUTO auto0.tap - use "... -irlen 4"
Warn : AUTO auto1.tap - use "... -irlen 4"
Warn : AUTO auto2.tap - use "... -irlen 4"
Warn : gdb services need one or more targets defined
```

Figure 3:

Ha anche trovato modalità diagnostiche attivabili direttamente dal cavo SATA (e quindi da un semplice software caricato sul computer, magari un malware) che permettono di eseguire operazioni equivalenti senza nemmeno estrarre l'hard disk dal computer, o saldarci e collegarci alcunché.

La prima funzionalità dimostrativa realizzata da Sprite_TM è stata quella di modificare il firmware del disco in modo che, se sul disco stesso fosse stato installato Linux, fosse possibile a qualsiasi utente collegarsi come "root".

E' sufficiente far arrivare all'hard disk, per esempio scrivendoci un file che la contenga, una stringa "magica", nell'esempio del seminario "HD, root", perché il firmware fornisca al sistema operativo un falso file di password, contenente la password di root scelta a piacere dall'utente. Un utente del sistema che contenga l'hard disk "taroccato" può cosi collegarsi come root e fare ciò che vuole. Il bello è che il file delle password per tutti gli altri utenti continuerà a contenere e mostrare la vecchia password. Una funzionalità del genere non può essere sradicata dall'hard disk riformattandolo o sovrascrivendone integralmente il contenuto.

Ma è stata la seconda funzionalità nascosta realizzata che ha fatto cadere la mascella a Cassandra e scatenato un applauso a scena aperta da parte di alcune centinaia di persone. Sprite_TM ha installato Linux "dentro" l'hard disk. Lo ripeto più lentamente, **d-e-n-t-r-o l'hard disk**, non sull'hard disk.

Niente a che fare quindi col sistema operativo che l'utente installa sull'hard disk, qualsiasi esso sia, e niente a che fare con la CPU del computer.Il Linux installato "dentro" l'hard disk è memorizzato in maniera nascosta, e viene eseguito dalla CPU "disoccupata" dell'hard disk. Nella semplice versione mostrata, può essere controllato ed utilizzato tramite la porta seriale dell'hard disk.

Inutile dire che il suddetto Linux è onnipotente nei confronti dell'hard disk stesso, ed invisibile a qualsiasi utente normale del computer, fosse pure un perito forense.

E su questa strada si potrebbe continuare immaginando un hard disk su cui si può innescare una lenta autodistruzione tramite l'invio di una stringa "magica", facendone corrompere poco alla volta il contenuto mentre l'ignaro possessore continua a lavorarci tranquillamente.

Oppure un hard disk a prova di copia, che può essere usato normalmente, ma che si "accorge" di una lettura sequenziale eseguita allo scopo di clonarlo, e gli fornisce contenuti falsi o, tanto per drammatizzare, cancella tutti i propri contenuti. E, ricordiamolo, stiamo parlando di cose che avvengono "dentro" l'hard disk, senza coinvolgere il computer a cui è collegato, e che nemmeno una riformattazione può sradicare.

Questa prima "Scheggia" termina qui. La paranoia era, resta e sarà sempre una virtù.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero